EV 318284575

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION FOR LETTERS PATENT

* * * * *

RADIO FREQUENCY SECURITY SYSTEM, METHOD FOR A BUILDING FACILITY OR THE LIKE, AND APPARATUS AND METHODS FOR REMOTELY MONITORING THE STATUS OF FIRE EXTINGUISHERS

* * * * *

INVENTORS

Larry Runyon
Wayne M. Gunter
Ronald W. Gilbert

ATTORNEY'S DOCKET NO. 12839-E CIP (BA4-198)

RADIO FREQUENCY SECURITY SYSTEM, METHOD FOR A BUILDING FACILITY OR THE LIKE, AND APPARATUS AND METHODS FOR REMOTELY MONITORING THE STATUS OF FIRE EXTINGUISHERS

CROSS REFERENCE TO RELATED APPLICATION

[0001] This is a continuation-in-part of U.S. Patent Application Serial No. 09/940,142 (attorney docket 12839-E), filed August 23, 2001, naming as inventors Wayne M. Gunter, Larry Runyon, and Ronald W. Gilbert, and which is incorporated herein by reference.

GOVERNMENT RIGHTS

[0002] This invention was made with government support under contract number DE-AC0676RLO1830 awarded by the U.S. Department of Energy. The Government has certain rights in the invention.

TECHNICAL FIELD

[0003] Aspects of the invention relate to a system, method and apparatus for maintaining security, and more particularly for maintaining security in an environment such as a building facility where there is a security-sensitive area with security-sensitive objects or items. Other aspects of the invention relate to fire extinguishing systems and methods, and to sensing, monitoring, and remote transmitting apparatus and methods used in connection with fire extinguishing equipment.

BACKGROUND OF THE INVENTION

[0004] The standards and requirements for fire extinguishing systems can be an overwhelming management task for Safety/Security Managers, who are

responsible for large buildings or facilities. For example, at the Mandalay Hotel in Las Vegas, Nevada, there are over 1900 fire extinguishers that require daily oversight and management. When one considers, for example, the following mandatory NFPA standards and requirements associated with fire extinguishers, it becomes readily apparent that the management of these systems in large buildings/facilities can be a monumental task:

1) Ensure fire extinguishers have not been tampered with or illegally removed,

2) Ensure fire extinguishers undergo required monthly, periodic and annual inspections to confirm they are fully charged and operable,

3) Ensure fire extinguishers undergo scheduled maintenance/testing (annual hydrostatic and conductivity testing, system recharging, etc.), and

4) Ensure fire extinguisher record keeping/documentation is completed.

[0005] Various fire extinguisher apparatus have been heretofore proposed. For example, U.S. Patent No. 6,125,940 to Oram (incorporated herein by reference) discloses a pressure indicating system for fire extinguishers whereby an audio alarm is sounded if the fire extinguisher is overcharged or undercharged. A visual indicator displaying the amount of pressure is also provided.

[0006] U.S. Patent No. 5,775,430 to McSheffrey (incorporated herein by reference) discloses a portable fire extinguisher, a valve assembly, and a gauge displaying the pressure condition of the fire extinguisher. An electronic circuit issues a signal in response to a condition, such as low pressure in the tank, smoke, lack of light, lack of external power, low battery, or lack of inspection

reset within a predetermined amount of time. Attention is also directed to the following patents to McSheffrey et al. which disclose similar systems and improvements and which are incorporated herein by reference: 5,848,651; 6,302,218; 6,311,779; and 6,488,099.

[0007] U.S. Patent Nos. 5,808,541, and 6,104,301, both to Golden (and both incorporated herein by reference), disclose an automatic fire suppression system having an electronic processor capable of monitoring system function, pressure, power level, and power source. A fire sensor and an audible or visual alarm are coupled to the processor. A valve is opened and the alarm is activated if the sensor detects a fire. A remote transmitter can be used to allow the system to be activated and the valve opened from a location remote from the hazard. A GPS device can be coupled to the processor and the location of the device can be communicated to a remote operator in the event that the presence of a fire is detected.

[0008] U.S. Patent No. 5,728,933 to Schultz et al. (incorporated herein by reference) discusses, among other things, the problem of determining if all the fire extinguishers in a building are properly charged. It discloses (starting, for example, at Col. 11, line 9) a remote sensing and receiving system that may be employed in fire extinguisher devices. A remote sensor unit, attached to a fire extinguisher device, communicates with a receiver unit 500 through infrared signals. The sensor unit must be capable of transmitting data, to the receiver unit, indicative of identification of the fire extinguisher. The sensor unit stores information in memory, such as building address, date of filling, filling sight, barometric pressure at filling sight, device identification number, and location inside the building. Pertinent information for extinguisher maintenance and

inspection could be stored in memory. In the normal course of building maintenance, an inspector holding a receiver unit periodically walks up to the fire extinguisher device and presses appropriate keys on a keyboard in order to activate the sensor unit. The sensor unit is turned on and transmits signals indicative of characteristics of the fire extinguisher device and the sensor unit. Such characteristics include current pressure in the extinguisher, identification of the fire extinguisher, date of charging, as well as other data stored by the sensor unit.

[0009] A commercial product, Fire Extinguisher Theft Stopper™, sounds an audio alarm when a fire extinguisher is removed from a designated position.

[0010] A fire extinguisher system is needed having improved sensing of fire extinguisher parameters and/or to assist with management of fire extinguisher systems.

SUMMARY OF THE INVENTION

[0011] Some embodiments of the present invention provide a method arranged to reduce security risks in or adjacent to a building facility where there are in, or proximate to, the building facility components which comprise one or more (or more than one) of the following:

a) building component(s) which are part of, or associated with, a building of the building facility;

b) facility component(s) which are in or adjacent to the building and relate to functions or occupancy of the building facility;

c) other component(s) which are in or adjacent to the building facility that are not included in building components or facility components.

[0012] Each of these components is further categorized as follows:

a) security-sensitive components which comprise:

i. component(s) which themselves are security-sensitive (i.e. because of having or containing security-sensitive information or items or components which are of sufficient value to be security-sensitive);

ii. component(s) which are of a nature that if moved or otherwise tampered with in some manner such tampering may indicate a security risk;

iii. components which are both themselves security-sensitive and also are of a nature that if moved or otherwise tampered with in some manner such tampering may indicate a security risk;

b) non-security-sensitive component(s), which include the items or components which are not security-sensitive.

[0013] In some embodiments, the method comprises providing at least one tamper-indicating device which in turn comprises a tamper-responsive section which comprises at least one tamper-responsive portion which has an intact condition and a non-intact condition. In a preferred form of the present invention, this tamper-responsive portion has an electrically conductive portion which in the intact position is able to conduct electricity between first and second

tamper related locations, and in the non-intact position is not able to conduct electricity between the first and second tamper related locations.

[0014] Also, in some embodiments, the tamper-indicating device comprises a signaling section that is operatively connected to the tamper-responsive section in a manner to:

a) provide a signal indicating at least one of;

I. a non-intact condition;

II. an intact condition; or

b) not provide a signal in response to an interrogating signal to indicate:

I. a non-intact condition; or

II. an intact condition

[0015] The tamper-indicating device is placed in a security risk detecting position by operatively engaging the tamper-indicating device to two of said components, at least one of which is a security-sensitive component. The two components are characterized in that relative movements between the two components indicates a possibility of a security risk occurrence. The tamper-indicating device is arranged and connected to the two components so that relative movement between the two components causes a break or damage to the tamper-responsive section to cause the tamper-responsive section to go to its non-intact condition.

[0016] Then a signal receiving device is operated to ascertain either a reception of a signal or a lack of reception of a signal from the tamper-indicating device to ascertain the possible security risk occurrence. In some embodiments of the present invention, the tamper-indicating device transmits its tamper-

indicating signal in response to the tamper-responsive section going to its non-intact condition. The tamper-indicating device has a sleep mode which exists so long as the tamper-responsive section is in its intact position. The tamper-indicating device is caused to go from the sleep mode to an active mode upon occurrence of the tamper-responsive section going to its non-intact condition to in turn to cause the tamper-signaling section to transmit the tamper-indicating signal. In the preferred embodiment the electrically conductive portion in the intact position causes the tamper-indicating device to remain in its sleep mode and in the non-intact position causes the tamper-indicating device to go to its active mode.

[0017] In a preferred form, the electrically conductive portion is operatively connected to circuitry of the tamper-signaling section in a manner that with the electrically conductive portion in its intact position, an input to a micro-controller of said tamper-signaling section is at a first voltage level. Then with the electrically conductive portion in its non-intact position, the input to the micro-controller is at another voltage level, with the change from the first voltage level causes the micro-controller to place the tamper-signaling section into its active mode.

[0018] In another embodiment of the present invention, interrogating signals are transmitted to the tamper-indicating device, and the tamper-indicating device modulates the signal in response to the interrogating signal so that a modulated response is transmitted when there is an intact condition of the tamper-responsive section. When a non-intact condition exists, the modulated signal is not transmitted, thus indicating a possibility of a security risk.

[0019] Also in some embodiments, the tamper-indicating device with the tamper-responsive section in its intact position is energized by an interrogating signal to provide a modulated response. With the tamper-responsive section in its non-intact position, the tamper-responsive device does not send the modulated response. In a specific form, the electrically conductive portion of the tamper-indicating device is operatively connected into circuitry of the tamper-signaling section so that when the tamper-signaling section is conductive, energizing current from the interrogating signal is able to cause the modulated response to the interrogating signal.

[0020] In a preferred form of the present invention the tamper-signaling section comprises operating components which are positioned within a housing of the tamper-signaling section. The operating components are responsive to the tamper-responsive section to produce the tamper-indicating signal. The tamper-responsive section comprises a plurality of tamper-responsive portions which are operatively connected to the tamper-signaling section in a manner that the signal transmitting section responds to any one of these tamper-responsive portions being in its intact or non-intact condition.

[0021] In a specific application of the present invention, a first connecting portion of the tamper-indicating device is connected to one of the two components, and a second connecting portion of the tamper-indicating device is connected to the other of the two components, with a tamper-responsive region of the tamper-responsive section being between the connecting portions in a manner that relative movement of the two components causes the tamper-responsive region to become severed or damaged to make the electrically conductive portion become non-conductive.

[0022] In some arrangements the two components have facing surfaces adjacent to one another, and the tamper-indicating device is positioned between the two facing surfaces. The first connecting portion of the tamper-indicating device is connected to one of the two components and the second connecting portion is connected to the other of the components in a manner that relative movement of the two components moves the two facing surfaces apart to cause a break or damage to the electrically conductive portion.

[0023] In other arrangements, there is a plurality of these tamper-indicating devices positioned between the two facing surfaces and connected to the facing surfaces, and the tamper-indicating devices are arranged so as to be positioned inwardly from surrounding edge portions of the surfaces so that relative rotational movement of the components to rotate the facing surfaces away from one another causes at least one of the tamper-indicating devices to go to its non-intact position. In another arrangement the first and second connecting portions of the tamper-indicating device are located on the tamper-responsive section, and the tamper-responsive section is connected to surface of the two components which are in general alignment with one another and spaced from one another.

[0024] Some aspects of the invention provide a method of remotely monitoring the status of multiple fire extinguishers, the method comprising coupling sensors to respective fire extinguishers in sensing relation to the fire extinguishers, the sensors each being configured to sense a parameter of the fire extinguisher to which it is coupled; associating transmitters with respective fire extinguishers, the transmitters being configured to selectively transmit information identifying the fire extinguisher with which the transmitter is

associated and to selectively transmit information indicative of the sensed parameter; providing a receiver in selective wireless communications with the transmitters; and providing a computer coupled to the receiver, the computer being configured to maintain testing schedules for respective fire extinguishers and being configured to provide an output when it is time for an extinguisher to be inspected, tested, or undergo maintenance, the computer also being configured to selectively store information from a plurality of the transmitters.

[0025] Other aspects of the invention provide a system for remotely monitoring the status of one or more fire extinguishers includes means for sensing at least one parameter of each of the fire extinguishers; means for selectively transmitting the sensed parameters along with information identifying the fire extinguishers from which the parameters were sensed; and means for receiving the sensed parameters and identifying information for the fire extinguisher or extinguishers at a common location. The sensed parameters may be, for example, removal of a trigger pin or movement of a fire extinguisher. Other systems and methods for remotely monitoring the status of one or more fire extinguishers are also provided.

BRIEF DESCRIPTION OF THE DRAWINGS

[0026] Preferred embodiments of the invention are described below with reference to the following accompanying drawings.

[0027] Fig. 1 is a schematic plan view of a building facility in which the system, apparatus and method of the present invention can be incorporated.

[0028] Fig. 2 is a semi-schematic plan view of a portion of a false ceiling where there are ceiling tiles supported by a plurality of support members, with

the tamper-indicating device of a first embodiment of the present invention shown in its installed position.

[0029] Fig. 3 is a plan view, as in Fig. 2, showing somewhat schematically one of the tamper-indicating devices of the present invention, having two tendrils.

[0030] Fig. 4 is a view similar to Fig. 3, showing a tamper-indicating device having four tendrils and being positioned at the juncture of corner portions of four adjacent ceiling tiles.

[0031] Fig. 5 is a schematic view showing the main components and circuitry of a first embodiment of the present invention.

[0032] Figs. 5A and 5B are each a schematic drawing of a passive tamper-indicating device similar to that shown in Fig. 5.

[0033] Figs. 6A, 6B and 6C are schematic views of second, third and fourth embodiments having other arrangements of a tamper-indicating device which would be useable in broader applications of the present invention.

[0034] Fig. 7 is a side elevational view, partly in section, showing a fifth embodiment of the tamper-indicating device.

[0035] Fig. 8 is a plan view of the tamper-indicating device of Fig. 7.

[0036] Fig. 9 is a side elevational view, partly in section, similar to Fig. 7, showing a sixth embodiment of the present invention.

[0037] Fig. 10 is a plan view showing three of the tamper-indicating devices of Fig. 9 positioned at the bottom surface of a security-sensitive object.

[0038] Fig. 11 is a side elevational view of the arrangement of Fig. 10, showing the three tamper-indicating devices positioned between the security-sensitive object and a support member, such as a table top.

[0039] Fig. 12 is a side elevational, partly in section, showing yet a seventh embodiment of the present invention.

[0040] Fig. 13 is a view similar to Fig. 12, showing an eighth embodiment of the present invention.

[0041] Fig. 14 is a side elevational view showing a couple of the tamper-indicating devices of Fig. 13 positioned under a security-sensitive item positioned on a support structure such as a tabletop.

[0042] Fig. 15 is a schematic drawing of a tamper-indicating device of a ninth embodiment of the present invention.

[0043] Fig. 16 is a side elevational view, partly in section, showing the tamper-indicating device of Fig. 15 in an operating position mounted into a security-sensitive object and positioned on a support structure such as a tabletop.

[0044] Fig. 17 is a top plan view showing a tenth embodiment of the present invention.

[0045] Fig. 18 is a view showing the portion of the tamper-indicating device of Fig. 17 with the elongated tamper-responsive section being in a rolled up configuration.

[0046] Fig. 19 is a plan view of a building facility, similar to Fig. 1, showing generally the same facility as shown in Fig. 1, but further showing components where the present invention is combined with a compatible security system.

[0047] Fig. 20 is a schematic view of the interrogation and control apparatus utilized in the combined system shown in Fig. 19.

[0048] Fig. 21 is a block diagram showing a fire extinguisher, sensors, and a transceiver of the system of Fig. 22.

[0049] Fig. 22 is a block diagram showing a system embodying various aspects of the invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

[0050] In Fig. 1, there is illustrated by way of example, an environment in which the system of the present invention could be used advantageously. Fig. 1 shows schematically a building facility which comprises a building structure 12 defining a secured area 13. The structure 12 comprises a floor 14, four sidewalls 16, 18, 20 and 22, and a ceiling (a portion of which is indicated at 24). The sidewall 16 has a doorway (exit/entrance) 26 for ingress and egress to and from the security-sensitive area 13 and an emergency exit doorway 28. The wall 18 has three windows 30 leading to an outside location.

[0051] Within the secured area 13, are a number of desks 32 which would normally be used by the personnel in the secured area 13 during working hours. By way of example, there is a locked safe 34 (or vault), three locked file cabinets 36 and two unlocked file cabinets 38, which are positioned adjacent against the wall 20. There is also shown somewhat schematically several security-sensitive items generally designated 40, and these would be various movable items which would quite commonly be in a security-sensitive area. These could include documents, written communications, computer hard drives, discs, and other computer information media, funds and currency, items which contain evidence or evidentiary data, high valued items, etc. However, in the non-working periods during which the security-sensitive area may not have any people therein, these security-sensitive items 40 will be placed either in the safe 34, one of the locked file cabinets 36 or some other secure location.

[0052] At this point it would be helpful for a more complete understanding of the present invention to indicate that the present invention can be combined with or incorporated with one or more other security systems. One such security system is described in U.S. Patent Application Serial No. 10/042,742, entitled "Radio Frequency Personnel Alerting Security System and Method", filed September 23, 2002, which is incorporated by reference herein. This other security system is particularly adapted for maintaining the security of the moveable security-sensitive items 40, as indicated above. Later in the present text this other security system will be summarized and it will be indicated how the two systems could be used in combination. Thus, the contents of this other above mentioned patent application are incorporated herein by reference.

[0053] To continue now with the description of the present invention, reference is again made to Fig. 1. There are the other objects or components indicated at 42, which are also security-sensitive either because of the information they contain or possibly for some other reason, such as being a rather expensive item which should be protected from theft. These could be, for example, computer related equipment, or a locked container which is used to contain security-sensitive documents and which for convenience is placed on a person's desk. These objects 42 are characterized in that either for reasons of size, or convenience, it is not practical (or desirable) to place these in a secured location, such as a safe 34 or the locked file cabinet 36.

[0054] Also, these objects 42 could be such things as the safe 34 and 25 the locked file cabinet 36. Even though these are securely locked, they could be susceptible to security risks by someone simply removing the entire safe 34 or locked file cabinet 36 from the security-sensitive premises. Then these could be

opened at some other location to remove the security-sensitive documents. Also, there are other security problems, such as unauthorized personnel making a covert entry through the building structure into the secured area. Aspects of the present invention relate to maintaining security for these sorts of items and situations.

[0055] With the above being given as further background information, there will now be described the various embodiments of the present invention.

[0056] A first embodiment of the present invention will now be described with reference to Figs. 1-5. As indicated previously in the introductory portion of this text under the subject heading "Background Art", there is one type of security problem where there is a security-sensitive area where the surrounding walls are not true floor to true ceiling walls, but extend only partially toward the true ceiling. Then there is a false ceiling made up of ceiling tiles which are supported by metal support members (beams) that extend in a grid-like pattern over the ceiling area at a location spaced downwardly from the true ceiling. Also (as indicated earlier in this text), in the prior art where that area with the false ceiling tiles is security-sensitive, in many instances the use of ceiling tile clips is required to be installed in the ceiling system. Then when any of these ceiling tile clips are disturbed (for example by a person moving or removing one of the ceiling tiles), visual inspection will indicate that this disturbance has occurred, thus indicating the possible occurrence of a covert intrusion. Both the initial installation of the ceiling tile clips and the regular visual inspection are costly. Also, if a covert intrusion has occurred, it may be many hours later that the visual inspection is made. This first embodiment is designed to alleviate this problem.

[0057] To describe now this first embodiment reference is first made to Fig. 2 which shows a portion of the aforementioned false ceiling 24, and specifically there is shown in Fig. 2 four of the individual ceiling tiles 46 supported by the support members formed in a rectangular grid pattern, these support members being indicated schematically at 48. Depending upon the size of the area of the false ceiling 24, there could be as many as several hundred tiles 46. These are arranged in a rectangular grid pattern, and the four tiles 46 that are shown in Fig. 2 are arranged in such a configuration, so that there is a juncture location 50 at which four adjacent corners 52 of the tiles 46 meet are closely adjacent to one another.

[0058] In accordance with the present invention, there is located at each of these juncture locations 50 a tamper-indicating device 54. This device 54 incorporates basic RFID technology, and in this particular embodiment comprises an operating or transmitting section 55 which comprises a containing housing 56, and a tamper-indicating section 57 which in this particular arrangement shown in Fig. 2 (and also shown in Fig. 4) comprises four elongate fingers or tendrils 58 which are operatively connected to the transmitting section 55. As shown herein, these four tendrils extend outwardly from the housing 56, with these tendrils 58 being oriented at right angles to one another. As can be seen in Fig. 2, each of these tendrils 58 reaches outwardly to extend over the corner portion 52 of a related ceiling tile 46. Each tendril 58 is bonded or otherwise secured to its related ceiling tile 46. If one of these ceiling tiles 46 is moved, as will be described later herein, the tendril 58 (which is attached to that tile 46) would break or otherwise be damaged so as to cause a separation or break of a frangible wire of the tendril 58.

[0059] When one of the tendrils 58 is so damaged, this causes the tamper-indicating device 54 to transmit an electromagnetic alarm signal (desirably an RFID signal which would identify that particular tamper-indicating device) to a suitable receiver/monitor indicated schematically at 59, which in turn provides a signal to cause remedial action to be taken (see Fig. 1). Such action quite likely would be an on site investigation at the location of signal producing RF tamper-indicating device or devices 54 to see if a covert intrusion has been made into the secured area.

[0060] In Fig. 4, there is shown an RF tamper-indicating device 54 which has four such tendrils 58, and in Fig. 3, there is shown another RF tamper-indicating device 60 having an operating section 61 with two tendrils 62 extending oppositely from one another. It can be seen in Fig. 2 that this RF tamper-indicating device 60 is used at a location where there are only two adjacent ceiling tiles 46.

[0061] The tamper-indicating device 54 and 60 can be considered as a specialized form of an RFID tag. Accordingly, in the following text, for convenience, the tamper-indicating device will often be referred to as a "tag", "RF tag", or "RFID tag".

[0062] While the first embodiment of the present invention has been described only with reference to the ceiling tiles 46, it is to be understood that it could be applied to other components of the building structure 12. For example, the windows 30 may be of a nature that these are seldom opened (or opened not at all), and yet these would present possible opportunities for a covert entry. The radio frequency tamper-indicating device 54 or 60 could be used with these in generally the same manner as indicated above. Also, there may be structural

panels or components which are joined together to form, for example, the walls or ceiling portions of some other design, and the radio frequency tags or members 54 and/or 60 could be used to provide security at those locations also.

[0063] To describe the components of the operating section 55 of the RF tag 54 or 60, reference is made to Fig. 5. In the text which follows, since the operating components of the tags 54 and 60 are identical (or substantially identical), reference will be made only to the tag 54 with the understanding that the description refers as well to the tag 60. These operating components are collectively designated as a signal generating apparatus, which is identified by the numeral 63. This apparatus 63 comprises a transceiver 64 that is operatively connected to an antenna 66. The transceiver 64 has the capability to transmit through the antenna 66 an electromagnetic signal to the receiver monitor 59 (see Fig. 1).

[0064] The transceiver 64 is also operatively connected to a micro-controller 68 (e.g., a microprocessor), such as the Texas Instruments MSP430 series or any other suitable processor, and has an operative connection at 70 to a battery 72 which in turn is connected to ground at 74. Any conventional transceiver 64 can be used as long as it is compatible with the micro-controller 68 and can be activated by a signal from the micro-controller 68. The micro-controller 68 is normally in a very low power "sleep mode" until activated. To activate the micro-controller 68 there is provided a connection at 76 to a resistor 78 that is in turn connected to a positive voltage terminal 79 from the battery 72. The connection at 76 also connects to the aforementioned frangible wire of the tendril 58. This frangible wire is indicated herein at 80 and (as indicated previously) is part of its related tendril 58. The other end of the frangible wire

connects to a ground at 82. In this particular embodiment, the frangible wire 80 extends in an elongate loop, and the connections at 76 and 82 are adjacent to the RF tag housing 56. The resistance level of the wire 80 is relatively low and the resistance level of the resistor 78 is relatively high. Accordingly, in the sleep mode very little current flows through the resistor 78, and the voltage at the connection 76 is essentially at ground.

[0065] To describe now the operation of the RF tag 54, as indicated above, the micro-controller (micro-controller) 68 is normally in the low power sleep mode. When a security breach breaks the frangible wire 80 in the tendril 58, this causes the connection at 76 to swing from a low voltage state to the voltage at the terminal 79 through the resister 78. This state causes an edge triggered interrupt within the micro-controller (micro-controller) 68, and the micro-controller in turn powers up from its sleep state and activates the transceiver 64 (functioning as a transmitter). The transceiver 64 then sends a signal through the antenna 66 to the receiver/monitor 59. This signal which is sent to the receiver/monitor 59 gives a message indicating that "I am damaged; my wire 80 has been broken or disconnected".

[0066] This particular type of RFID tag (tamper-indicating device) 54 described in reference to Fig. 5 is constructed so that in the sleep mode almost no charge is required to maintain the alert condition of the device 54, and the device 54 could be operational in its sleep mode, for as long as possibly two years or more. At that time, another battery could be installed, or assuming the cost of the RF tag 54 is sufficiently low cost, a new tag 54 could be installed.

[0067] Alternatively, this system could be arranged so that the tamper-indicating devices 54 and 60 would be made as passive RFID tags where the tag

54 or 60 would not have a power source as a battery 72, and the power of an interrogation signal would be sufficient to generate the response as needed from the tag 54 or 60. In this instance the tags 54 and 60 would likely be arranged so that when interrogated, when the tag 54 or 60 is intact (i.e., the wire 80 is not broken), the tag 54 or 60 would give an "I'm okay" response. On the other hand, when the tag 54 or 60 is interrogated and no response is received, then this lack of a response would be interpreted as indicating that the tag 54 and 60 is inoperative (which would usually mean that the wire 80 is broken or damaged.

[0068] The tamper detecting device 84 by which this could be accomplished is shown schematically in Fig. 5A. There is a receiving antenna 86, operatively connected to one end of the wire loop 80, with the other end of the loop 80 being connected to an input 87 of the operating circuitry 88 which would include the micro-controller and other related components. The output of the operating section 88 connects to a transmitting antenna 90 from which the modulated return signal is directed back to the interrogating/receiving location or simply back to one or more receiving locations. The operating section 88 would be activated by the energy that the receiving antenna 86 absorbs from the interrogating signal and modulates this in a manner that the modulated signal would travel from the transmitting antenna 90 back to the receiving location.

[0069] In operation, when the wire 80 is intact, the interrogating signals would generate a modulated response that would be received as an "I'm okay" signal. Since the modulated response identifies that particular tag 54, this response will be interpreted as coming from a particular tag location. On the other hand, when the wire 80 is broken, the power from the interrogating signal is not transmitted from the receiving antenna and no response is generated from

the operating section 88. Thus, the transceiver/monitoring apparatus would recognize that no response was given to that interrogated signal and this would indicate that the wire 80 at this particular tag was broken, and thus indicating a possible security risk occurrence.

[0070] A modified version of the device is shown in Fig. 5B. The components of the device shown in Fig. 5B which are the same as or similar to components of the tamper-indicating device 84, Fig. 5A, will be given light numerical designation with a (') designation distinguishing those of this modified version of Fig. 5B. The tamper-indicating device 84' of Fig. 5B and comprises the same antennas 86' and 90', the circuitry 88', and the wire loop 80'. However, the wire loop 80' is not connected in series between the antenna 86' and the circuitry 88'. Rather, the wire loop is connected to the circuitry 88' and its intact and non-intact configurations are detected in the manner described previously herein relative to the embodiment shown in Fig. 5. Also, the receiving antenna 86' has a direct connection at 87' to the circuitry 88'. The return signal from the circuitry 88' is, as in the circuitry of Fig. 5A, transmitted to the transmitting antenna 90'.

[0071] Within the broader scope of the present invention, there could be a number of variations. Three of these are shown as additional embodiments in Figures 6A, 6B and 6C.

[0072] Initially the second embodiment shown in Fig. 6A will be described. In describing this second embodiment, components of the second embodiment which are essentially the same as (or similar to) components of the first embodiment will be given like numerical designations, with a "a" suffix distinguishing those of the second embodiment. The tag in the embodiment of

Figure 6A is the same as shown in Fig. 5, in that there is the transceiver 64, the antenna 66, the micro-controller 68, and the battery 72, as shown in Figure 5 (not shown in Fig. 6A).

[0073] Accordingly, only those components of the second embodiment shown which function somewhat differently or are in a somewhat different arrangement are illustrated in 6A.

[0074] In Fig. 6A, there is the connection 76a to the micro-controller (68 in Fig. 5), and there is also the voltage source 79a which connects to the connection 76a through the high resistance resistor 78a. However, instead of having the frangible wire 80, there is provided a thermistor 92a connected to the connection 76a and to the ground connection 82a. This thermistor 92a normally is conductive, but if the ambient temperature rises above a predetermined level, the electrical resistance increases. Accordingly, this will initiate a signal to the micro-controller 68 which will in turn transmit an alarm signal that there is a high temperature condition at the thermistor 92a, this high temperature condition possibly resulting from a fire.

[0075] In Fig. 6B, there is shown a third embodiment, and as in the description relative to the embodiment of Fig. 6A, the components of this third embodiment which correspond to components in the first and/or second embodiments will be given like numerical designations, but with a "b" suffix distinguishing those of the third embodiment.

[0076] This RF tag of the third embodiment is somewhat similar to the second embodiment of Fig. 6A, but it differs in that the resistor 78b is connected between the connecting points 76b and 82b. Then there is located between the voltage source 79b and the connection 76b a phototransistor 94b. The

phototransistor 94b is normally nonconductive, but when a light is shone upon the phototransistor 94b, it then becomes conductive. Accordingly, it can be seen that in normal operation (when there is no light directed to the phototransistor 94b) the contact 76b will be at ground potential. Then when the phototransistor 94b becomes conductive, thus forming a conductive path from the points 79b to 76b, this activates the micro-controller to cause the alarm signal to be generated. For example, this RF tag could be located in a dark room, and if an anomalous light source is detected, this would create an alarm signal.

[0077] This third embodiment could be used in a variety of situations, and these are discussed further later in this text. However, to give one example at this time, the light sensitive surface of the photoresister could normally be covered by an opaque cover in an environment where there is light. The security intrusion or movement of security-sensitive item would result in the opaque cover being removed from the light sensitive surface, thus triggering an alarm.

[0078] Fig. 6C shows a fourth embodiment, and components of this fourth embodiment which are similar to prior embodiments will be given like numerical designations with a "c" suffix distinguishing those in the fourth embodiment. This RF tag 54 of the fourth embodiment is substantially the same as the third embodiment of Fig. 6B, except that in place of the photo transistor 94b, there is provided a magnetic reed switch 96c which is normally open. Then when the switch 96c comes in proximity to a source 97c of a magnetic field, then the switch element 98c closes. An application of this embodiment (in a somewhat modified form) will be described later herein.

[0079] Reference is now made to Figs. 7 and 8 which show a fifth embodiment. In describing this fifth embodiment of Figs. 7 and 8, components

which are similar to corresponding components in one or more of the prior embodiments will be given a like numerical designation or designations, with a "d" suffix distinguishing those of the fifth embodiment.

[0080] Fig. 7 is a side elevational view where there are shown two objects 100d and 102d, with these having first parallel and aligned surfaces 104d and 106d, respectively, aligned in a common plane, and two other parallel surfaces 108d and 110d which face one another and are spaced laterally from one another, with the surfaces 104d and 108d being at right angles to one another and meeting at a corner edge 112d, and the surfaces 106d and 110d also being at right angles to one another and meeting at an edge location 114d. These two objects 100d and 102d could be two building structural components which are adjacent to one another, or the object 100d could be stationary structure, and the object 102d could be a security-sensitive container or some other security-sensitive object which is moveable and adjacent to the stationary structure 100d. Or these two members or components 100d and 102d could be two moveable objects which in a normal configuration would be adjacent to, or at least contiguous to, one another, but or of such a nature that when one of these is moved relative to the other, this would indicate an occurrence that may relate to a security risk.

[0081] With further reference to Figs. 7 and 8, the radio frequency tag or member 54d comprises a housing 56d containing the operating components and one arm or extension member 58d which is comparable to the tendril extension member 58. The housing 56d has at its bottom surface an adhesive coating 116d, by which the housing 56d can be securely bonded to the surface 106d. The tendril or arm 58d has two portions, namely a first portion 118d which is

directly connected into the housing 56d, and a second portion 120d which is at the outward end of the tendril 58d (i.e., further from the housing 56d). The two tendril portions 118d and 120d are joined to one another along a serrated or otherwise weakened juncture line or location 122d so that the two sections 11 8d and 120d can be more easily separated from one another at the location 122d.

[0082] There are provided a pair of stiffening plates, 124d and 126d. The stiffening plate 124d is fixedly connected (e.g., by bonding) to the tendril portion 118d, and the other stiffening plate 126d is fixedly attached (e.g., bonded) to the tendril portion 120d. These two plates 124d and 126d have adjacent edges 128d which are positioned closely to one another on opposite sides of the serrated or weakened location 122d.

[0083] In the plan view of Fig. 8, it can be seen that the tendril 58d comprises the wire loop 80d embedded into a rather thin elongate strip of material 130d. This could be plastic material or a plastic/fabric material could be similar to a piece of adhesive tape. The lower surface of the two tendril portions 124d and 126d each have an adhesive layer 132d and 134d, respectively, by which the tendril portions 126d and 124d are bonded to their respective upper surfaces 106d and 104d.

[0084] To describe the operation of this fifth embodiment of Figs. 7 and 8, it should first be noted that the two rigid plates 124d and 126d are each bonded to their respective tendril portions 118d and 120d that are in turn bonded to the surfaces 106d and 104d of the objects 102d and 100d so that two rigid plates 124d and 126d and the tendril portions 118d and 120d are fixedly connected to their respective objects 100d and 102d. Thus, when there is even a slight

relative movement between the two objects 100d and 102d, there will be a break occurring along the serrated location 122d of the tendril 58d.

[0085] To describe now the sixth embodiment of the present invention, shown in Fig. 9. As with the prior embodiments, components which are similar to the components of the prior embodiments will be given like numerical designations, with an "e" suffix distinguishing those of this sixth embodiment.

[0086] In Fig. 9 the RF tag or member 54e is positioned between two objects 100e and 102e, having facing flat surfaces 106e and 108e - which are closely adjacent to one another, with only the thickness of the RF tag 54e separating the two surfaces 106e and 108e. The object 100e could be, for example, a table top or a counter top, and the object 102e, could be, for example, a security-sensitive item such as a piece of computer equipment, or possibly a locked container which itself contains security-sensitive items.

[0087] This RF tag 54d has a housing 56e and a single tendril 58e. The overall configuration of this tag 56e can be the same as, or substantially the same as the tag 54d of the fifth embodiment.

[0088] The housing 56e is for the most part located adjacent to, but spaced laterally from, the object 102e so that its antenna is not shielded by the object 102e. The housing 56e has on its lower surface an adhesive layer 116e so as to be bonded to the surface 106e, and the upper surface of the tendril 58e has an upper adhesive surface 134e so as to be bonded to the surface 108e. In addition, the tendril 58e has bonded to its lower surface a rigid plate member 126e. There is a serrated or weakened portion 122e in the tendril 58e at a location closely adjacent to the housing 56e.

[0089] To describe the operation of this sixth embodiment, reference is now made to Figs. 10 and 11. Let us assume (as suggested earlier) that the lower member 100e is a table top and the object 102e is a piece of computer equipment which is security-sensitive. Further, it is expected that the piece of computer equipment 102e is to remain at a stationary location on the table top 100e for an extended length of time. To accomplish this, a plurality of the RF tags 54e are placed at spaced locations along the bottom surface 108e of the object (e.g., computer equipment) 102e, so that the top adhesive layer 134 sticks to the lower surface 108e of the computer equipment 102e. Then the piece of computer equipment 102e is placed on the top surface 106e of the table top 100e so that the bottom adhesive surfaces 116e of each of the housing portions 56e of the three RF tags 54e adheres to the upper surface 106e of the table top 100e. The adhesive layer 116e and 134e could initially be covered by a removable protective layer.

[0090] Now let us assume that someone wishes to remove this piece of computer equipment 102e from its position on top of the table 100e. Obviously, if the person simply lifts the computer equipment 102e from the table, each of the housing sections 56e of the three tags 54e will adhere to the upper surface 106e of the table top 100e, and the tendril sections 58e of each of the tags 54e will adhere to the piece of computer equipment 102e. This will cause the wire loop 80 and each of the tendrils 58e to break, with the RF tags 54e giving the alarm signal.

[0091] Now let us take the situation where the thief is aware of the use of the RF tags, and the thief attempts to somehow sever the adhesive layers 116 that adhere to the surface 106e or possibly the adhesive layers of the tendril

portions 58e that adhere to the bottom surface of the computer equipment 102e. Let us further assume that this person is successful of slipping a very thin severing tool underneath the computer equipment 102e. It is likely that this attempt to sever, for example, the RF tag 54e on the right side of Fig. 11 will raise the right side of the computer equipment 102e at least a short distance. This would cause the computer equipment 102e to rotate at least slightly about the left RF tag 54e so as to tend to raise at least one of the other RF tags 54e slightly above the surface 106e. The effect of this would be to separate the housing 56e from the tendril portion 58e along the severance line 122e, thus causing the alarm signal to be given.

[0092] A seventh embodiment of the present invention is shown in Fig. 12. As in the description of the other embodiments, components of earlier embodiment will be given like numerical designation with the "f" distinguishing those of this seventh embodiment.

[0093] An examination of Fig. 12 will indicate that the RF tag 54f of this seventh embodiment is very similar to the fifth embodiment, except instead of having a single tendril section 58e, there are two oppositely extending tendril sections 58f.

[0094] Thus, there is the central housing section 56f and the two aforementioned tendril section 58f on opposite sides thereof. There is a top adhesive layer 134f over the top surface of each of the tendril sections 58f. Also, the lower surface of the housing 56f has an adhesive layer 116f.

[0095] Also, there are two rigid plates 124f and 126f bonded to the related tendril members 58f so that the lower surface of these two rigid plates 124f and

126f are in the same plane as the lower adhesive layer at 116f of the housing 156f.

[0096] The operation of this seventh embodiment of Fig. 12 is similar to the operation of the sixth embodiment of Figs. 9-11. The particular application of this seventh embodiment could be used in other ways. For example, the two tendril sections 58f could be positioned beneath adjacent objects, so that either of the objects connected to their respective tendril sections 58f would activate the operating section contained in the housing 56f. Also, it may be that the object in which the tamper-indicating device 54 is attached has a somewhat different configuration where there are two side sections (e.g., where there is a U-shaped configuration in plan view). Then the housing section 56f could be placed in an open area between the two branches of the U, and the two tamper-indicating sections 58f could be under two side portions of the object to which the tamper-indicating device 54 is secured. In that instance, it could be that the tamper-indicating sections 58f could be spaced further from one another, or the center-located housing section 56f could be made at a greater length so as to extend further laterally.

[0097] An eighth embodiment is illustrated in Fig. 13. As in the description of prior embodiments, the components which are the same as, or similar to, components of any of the prior embodiments will be given like numerical designations, and in this instance, with a "g" suffix distinguishing those of this eighth embodiment. The depth of the RFID tag 54g is exaggerated for purposes of illustration.

[0098] The tag 54g comprises a housing 56g having a single tendril 58g extending outwardly therefrom. The bottom surface 140g of the housing 56g

and the bottom surface 141g of the tendril 58g each have the same adhesive layer 142g that bonds both the housing 56g and the tendril 58g to the underlying surface 106g.

[0099] At the outer portion of the tendril 58g (i.e., further from the housing 56g) there is an additional tendril component 144g positioned immediately above an outer portion of the tendril member 58g, and this tendril component 144g has its lower surface bonded to the upper surface of the outer portion of the tendril 58g by a bonding layer 146g. The upper surface 148g of the upper tendril component 144g has a bonding layer 150g.

[0100] The wire member 80g has two first wire portions 152g which extend from the housing 56g through the main tendril member 58g and at the outer portion of the tendril member portions 152g, these two wire members 152g take an upturn at 154g to extend into the upper tendril component 144g. Then there is a connecting wire portion 156g which connects to the upper ends of the tendril portions 154g. Thus, these wire portions 152g, 154g and 156g form a continuous loop.

[0101] The lower bonding layer 142g and the upper bonding layer 148g make relatively strong bonds, while the intermediate bonding layer 146g makes a relatively weak bond.

[0102] To describe the operation of the eighth embodiment, reference is now made to Fig. 14, where it shows a pair of the RF tag members 54g positioned on a surface 106g of a table 100g, and there is shown an object, such as computer equipment 102g having a lower surface 108g. The lower surface 108g of the computer apparatus 102g is bonded to the upper bonding layer 148g, and the lower surface 140g of the housing 56g and the lower surface 141g

of the tendril member 58g are bonded directly to the table surface 106g by the bonding layer 142g.

[0103] Let us now assume that someone is attempting to remove the computer apparatus 102g and also that this person recognizes that there may be some sort of security member between the apparatus 102g and the support member 100g. This person may simply wish to slide the computer member 102g over the table surface 106g in the hopes of foiling the action of the security member. However, with the arrangement of this eighth embodiment, the upper adhesive layer 148g will adhere strongly to the computer member 102g, while the lower bonding layer 142g will adhere strongly to the table top 106g. However, the relatively weak intermediate bonding layer 146g will give way and the upper tendril component 144g will slide laterally relative to the tendril member 58g. This will sever the two wire portions 154g.

[0104] Also, if it is attempted to raise one end of the computer apparatus 102g then again the upper tendril member 144g will separate from the lower tendril member 58g, also breaking the wire sections 154g. As in the previous embodiments, this will cause the operating components within the housing 56g to signal the alarm.

[0105] A ninth embodiment of the present invention is illustrated in Fig. 15 and 16. As in the description of prior embodiments, the components of this ninth embodiment which are the same as, or similar to, components of the earlier embodiments will be given like numerical designations, but with an "h" designation distinguishing those of this ninth embodiment.

[0106] It is contemplated that within the broader scope of the present invention, the tamper-indicating section 57 of the first embodiment could utilize

some component other than the wire 80, as shown in the 25 first embodiment and other embodiments. Such an arrangement is shown in this ninth embodiment.

[0107] In Fig. 15, substantially the same circuitry is shown as in Fig. 5, except that instead of having the wire 80 of the tendril, there is shown a magnetic reed switch 96h, such as shown in Fig. 6c. However, instead of having the magnet 97c of Fig. 6c as being itself a magnet, there is shown a magnetically permeable member 97c which is closely adjacent to the magnetic reed switch element 98h, with this magnetically permeable member 97h being part of the RF tag 54h.

[0108] To explain the operation of this ninth embodiment, reference will now be made to Fig. 16. In Fig. 16 there is shown a stationary support structure 100h, which could be, for example, a counter top or a floor of a structure. This structure 100h has formed in its upper surface a recess 162h, and there is positioned in the lower part of this recess 162h a permanent magnet 164h. The RF tag or member 54h is arranged so that the magnetically permeable member 97h is positioned at the lower part of the housing 56h, and the magnetic reed switch 96h is positioned immediately adjacent to the magnetically permeable member 97h. Further, the housing 56h is shown as fitting into a recess 162h formed at the lower surface 108h of the security-sensitive object 102h (which as in prior embodiments could be a container with security-sensitive documents, computer equipment, etc.).

[0109] With the object 102h (e.g., a security-sensitive container) being positioned on the surface 106h of the support structure 100h, the lower portion of the housing 56h of the RF member 54h extends downwardly a short distance

into the recess 162h. In this location, the magnetically permeable member 97h is in contact with the magnetic member 164h. (As shown in Fig. 16, there is a small gap between the magnetically permeable member 90h and the permanent magnet 164h, and this is simply being done for purposes of illustration to indicate that these are separate members).

[0110] Thus, the magnetic flux of the permanent magnet 164h permeates the magnetically permeable member 90h to in turn cause it to simply function as an extension of the magnet 164h and thus bring the reed switch 98 to its closed position. The magnetically permeable member 97h is made up of a magnetically permeable material which does not have "magnetic memory". Accordingly, as soon as the object 102h is moved upwardly so as to also lift the RF tag 54h, the air gap that is formed between the member 97h and the magnet 164h is created, with the magnetic flux in the member 90h decreasing substantially so that it is not able to maintain the switch member 98h in its closed position. Thus, when the switch 97h moves to its open position, this immediately sends a signal to the micro-controller to in turn produce an alarm signal.

[0111] Also, it is to be recognized, as with at least some of the other embodiments, that it is possible to arrange the RF tag 54h so that it responds to an interrogating signal, in which case a modulated response is made by the RF tag 54h to provide an "I'm okay" signal to the interrogating apparatus. In that case, when the object 102h is in a secured position, with the switch element 98h with the switch 80h being in its closed position (as shown in Fig. 16), it will be interrogated periodically and give the "I'm okay" signal, and then will not respond when the object 102h is moved out of its secured position of Fig. 16. But when

the modulated response is not received, this indicates a possible security risk occurrence.

[0112] A tenth embodiment is shown with reference to Fig. 17 and 18. As with the description of the prior embodiments, components of this tenth embodiment which are similar to components of prior embodiments will be given like numerical designations with a "k" suffix distinguishing those of this tenth embodiment. This tenth embodiment utilizes an RF tag 54k, which is the same as the RF tag 54 of the first embodiment, where the wire extends from the contact point 76 to a ground location. In this tenth embodiment, instead of utilizing the wire 80k in a relatively short tendril 58, the wire 80k extended outwardly for a more substantial length, such as ten feet, twenty feet, etc., up to the limit permitted by the design. Conceivably, the length of this wire could even be one hundred feet or several hundred feet. This wire 80k could be formed as two wires having the outer ends connected to form a - loop, or a single wire where the far end of the wire would simply be attached to a common ground with the RF tag 54k.

[0113] Part of the length of this wire 80k is shown, and there is illustrated schematically fasteners 170k at spaced locations also the wire 80k. These fasteners could be small adhesive strips. Also the wire 80k could be in or bonded to a plastic or fabric strip 171k with serrated "break" locations 172k at spaced intervals along its length where the wire 80k could be more easily broken.

[0114] It is apparent that if the break is made anywhere along the length of this wire 80k, this will cause the RF tag member 54k to send an alarm signal. One possible use for this tenth embodiment is, for example, where there is a

location with various security-sensitive objects which would need to be made secure in a very short time. This strip 171k with the wire 80k and with its fasteners 170k could be wound up in a roll as shown at 176k in Fig. 17, and as the wire 80k with its attached strip 171k is unwound from the roll 176k, it could be wrapped over, across or around various objects, and also across openings of various sorts to create a more secured environment.

[0115] A possible modification of this tenth embodiment is that portions of this plastic strip are made with a bottom adhesive layer which is made with a rather high bonding strength in areas where there are the serrated break locations 122k arranged at spaced locations along the strip portion 172k. The bond strength of the adhesive layer is sufficiently strong so that if one section 174k between two break lines 122k is pulled up, the adjoining sections 174k would still adhere to the substrate, and the wire 80k would break at the break locations 122k. Thus, if an intruder is attempting to carefully remove the wire with the strip 172k carefully to avert detection, as soon as the person raises one of these sections 174k the break will occur and thus the alarm signal will be given.

[0116] At such time as they need for security in this particular location passes, then the information would be given to the control system that the alarm signal from the tag 54k would be disregarded so that the wire 80k with the many fasteners 170k and the strips 172k could all be removed from that temporarily secured area without triggering the alarm system.

[0117] It was indicated earlier in this text that the system of the present invention could advantageously be incorporated into one or more other security systems, and the one system in particular which was mentioned is described in

the U.S. patent application entitled "Radio Frequency Personnel Alerting Security System and Method", naming the same inventors as in the present patent application.

[0118] The manner in which this is done will now be described with reference to Figs. 19 and 20. It will readily be recognized that Fig. 19 shows substantially the same building facility as shown in Fig. 1, but with a few additions. The components shown in Fig. 19 which are the same as (or similar to) those shown in Fig. 1 will be given like numerical designations, but with the numeral "2" preceding the numerals that appear in Fig. 1. Thus, the building facility is designated 210 the building structure is designated 212, the desks are designated 232, the safe designated 234, etc.

[0119] With regard to the items which have been added to Fig. 19 and which do appear in Fig. 1 are several RFID tag members 241, each of which is shown being associated with a security-sensitive item 240. It will be recalled that earlier in this text it was indicated that these security-sensitive items 240 are items such as documents, computer discs, and other moveable items, which in their secured position are either locked in the vault 234 or locked in the file cabinets 236.

[0120] However, during working hours when authorized personnel are present in the secured area 213, the security-sensitive items 240 could be outside of the secured location and, for example, on a person's desk. There is also shown a monitoring and interrogation apparatus 244 which is operatively connected to one or more antennas. Four such antennas are shown at 246 and broken lines are shown at the top of Fig. 19 to indicate the operative connection of the two antennas 246 at the top of the page to the monitoring and

interrogation apparatus 244. The two antennas 246 at the bottom of Fig. 19 have similar operative connections, but which are not shown for ease of illustration.

[0121] During non-working hours, during which the security-sensitive items 240 should be kept in a safe place, as indicated above, these items 240 could be kept either in the safe 234 or the locked file cabinets 236. Both the safe 234 and the locked file cabinets 236 are made of metal, and thus substantially block electromagnetic radiation or signals in the area.

[0122] To describe now the operation of the system of this additional security system, the monitoring and interrogation apparatus 244 sends out electromagnetic interrogation signals periodically through antennas 246 into the secured area 213. Each of the security-sensitive items 240 has attached to it an RFID tag 241, and with these sensitive security documents 240 being in the open, the interrogation signals will reach the RFID tags. Each tag 241 will send a response indicating- "I am in an open area and not in my secured location". Now let us assume that the security-sensitive items 240 are locked in the safe 234 or the file cabinets 236. Then when the interrogation signals are sent out, there will be no reply from the RFID tags 241, and thus the interrogation and monitoring system 244 would recognize this as indicating that the items 240 are in their secured locations.

[0123] Let us take now a situation where the authorized personnel are in the building facility and working at their respective desks 232 and various documents 240 are on the desks of these persons. When the noon hour comes and all of the personnel in the secured area 213 are to leave for lunch, all of the security-sensitive items 240 should be placed in either the safe 234 or the locked

file cabinets 236. Also the safe 234 and file cabinets 236 should be locked and RFID tags would be operatively connected to the locking mechanisms to indicate either a locked or unlocked condition. At this time the interrogation and control apparatus 244 would be sending out its interrogating signals. If no response signals are received, this would mean that all of the security-sensitive items have been placed in the safe 234 or file cabinets 236, and that these have been locked.

[0124] However, let us assume that at the noon hour the interrogation and control apparatus 244 sends out its series of signals to each of the RFID tags 241 and receives a response from one or more of these tags 241, thus indicating that security-sensitive items are left in a non-secured location. When this occurs, the apparatus 244 sends the appropriate alarm signals to initiate precautionary action. This occurs as follows.

[0125] As soon as any one of the personnel in the security-sensitive area 213 approaches the exit door 226, a proximity detector 248 recognizes that one or more persons is about to leave the area 213 through the door 226. The proximity detector 248 signals this to the apparatus 244 which immediately sends alert signals to alert the personnel who are about to leave the area through the door 226 to the fact that the area 213 is not secure since some of the documents 240 or other security-sensitive items 240 are left out in the open. This alert signal is telling the personnel not to leave the secured area until proper steps should be taken to make sure these documents or other security-sensitive items 240 are placed either in the safe 234 or the file cabinets 236. When this is accomplished, and when the personnel approach the door 226, there are no such alarms given.

[0126] The alarm could be a visual display 250, or an audio alarm 252 (vocalizing words or some sort of other alarm signal), or both. Also, it could be that in addition to giving the alert signals access through the door would either be impeded or blocked in some manner, such as by the apparatus 244 activating a lock 254 on the door. Or there could be a mechanism which would simply impede opening the door 226 to give a physical signal to the personnel that that person should not be leaving the area. If the person would leave the area regardless of these alert signals, then another alarm signal (indicating a more urgent alarm) could be given and appropriate security measures being taken.

[0127] Then during the non-working hours, the interrogation and control apparatus 244 could still function to send out its interrogation signals to see if any of these security-sensitive documents 240 are being removed from their security-sensitive locations (either in the safe 234 or the locked file cabinets 236). If this is detected, then this would indicate that there has possibly been a covert entry into the secured area 213 and either the safe or the locked file cabinets 236 have been tampered with.

[0128] Other features of this system being described in Fig. 19 are contained in the full text of the other patent application (these naming the same inventors as in the present patent application). Since these are incorporated by reference to such patent application, these will not be repeated in this text.

[0129] Reference is now made to Fig. 20, which shows schematically the main components of the interrogation and control apparatus shown in the other patent application. More specifically, there is indicated the motion detector (or other proximity detector) 248, the two displays 250 and 252, and also the antennas 246 and the lock or locks 254. There is a micro-controller 256 which is

operatively connected to the RF interrogator 258 that in turn sends interrogation signals through the antennas 246. The motion detector 244 gives its input to the micro-controller 256 and the response to the interrogation signals come back through the antennas 246, and through the interrogator 258 back to the micro-controller. Other inputs are provided from the various sources, which are indicated schematically and collectively at 260.

[0130] As indicated above, this system shown in Figs. 19 and 20 could be incorporated with the system of the present patent application, since the very same interrogation system and the antennas 246 could be used to send out the interrogation signals as needed, and also to receive the various alarm signals or "I'm okay" signals which would result from utilizing the system of the present invention.

[0131] Also, it becomes readily apparent from reviewing the operations of the present invention and also that the system of Figs. 19 and 20 that these two systems complement each other in that these are directed to related but somewhat different security risks. Thus with these two systems working cooperatively with one another, the overall security of the area is enhanced.

[0132] With the system of the present invention and the system from the aforementioned U.S. Patent Application being combined, the interrogation and control apparatus 244 would also serve the function of the receiver/monitor 59 of the present invention. This interrogation and control apparatus would act as a receiver of signals from those tamper-indicating devices 54 or 60 which are able to generate and transmit the signal without any interrogation. However, for those embodiments of the tamper-indicating devices of the present invention which are passive and respond to an interrogating signal, then the interrogation and control

apparatus 244 would be sending the interrogating signals and either be expecting a response or expecting no response for the items that are in the "I'm okay" condition.

[0133] In a preferred embodiment, the interrogating signals are sent sequentially and the interrogation is specific to each of the RFID tags or tampering indicating devices that are being monitored. Also the interrogation and control apparatus would have stored at its database the location of each tamper-indicating device (RFID tag) and the item or at least the type of item to which the tamper-indicating device (tag) attached or associated, and also its location. Therefore when the interrogations are made for the tags 241 that are associated with the security-sensitive items 240 (which should be available for interrogation only during certain periods) when the interrogating signals are sent, this would indicate the following.

[0134] During those periods where the security-sensitive items 240 are expected to be out of the locked file cabinets 236 or safe 234, then the response would be indicated as a signal indicating "I am present in the area of interrogation and therefore have not yet been taken out of this secured area". Further, if no response is received during the time periods where the items 240 are supposed to be in their secured location, the lack of a signal would indicate that these are in the safe 234 or the locked file cabinets 236. On the other hand a response during these periods where these items 240 are supposed to be securely placed in the file cabinets 236 and 234 would indicate a security risk occurrence.

[0135] With regard to the items 242, as indicated above for the some of the tamper-indicating devices, such as the device 54 of the present invention,

the interrogation and control apparatus 244 may never receive a signal from those items 242, since they would not have been tampered with and their tamper-indicating devices would remain in the intact position. For other items 242 which have their tamper-indicating devices or RFID tags passive, then a response would be a expected, and this would be a signal indicating "I'm okay; my tamper-responsive section is intact". On the other hand, a lack of a signal in response to an interrogation from the passive RFID tags would indicate that the tamper-indicating device 54 was in its non-intact position and would indicate a possibility of a security risk occurrence.

[0136] Figs. 21 and 22 show a system 310, embodying various aspects of the invention, for remotely monitoring the status of multiple fire extinguishers. The system 310 comprises a plurality of sensors adapted to be coupled to respective fire extinguishers 312 in sensing relation to the fire extinguishers 312. The sensors are each configured to sense a parameter of the fire extinguisher 312 to which it is coupled. In the illustrated embodiment, at least some of the fire extinguishers 312 have associated therewith a motion sensor 314 configured to sense if the fire extinguisher is moved.

[0137] In some embodiments, one or more fire extinguishers 312 have associated therewith an enable or trigger pin sensor 316 configured to sense if a fire extinguisher enable pin (trigger pin) is removed or tampered with. More particularly, in some embodiments, the trigger pin sensor 316 is defined by a tamper indicating device as described above in connection with Fig. 5, 5A, 5B, 6A, 6B, 6C, 7, 8, 9, 10, 11, 12 or 13, for example.

[0138] Still further, in the illustrated embodiment, at least some of the fire extinguishers 312 have associated therewith a pressure sensor 318 configured to sense fire extinguisher pressure (e.g., to determine if the fire extinguisher 312 is overcharged or undercharged).

[0139] The system 310 further includes a plurality of transmitters 320 (and internal or external antennas 321) associated with respective fire extinguishers 312. The term "transmitter," as used herein, is intended to encompass devices that are selectively polled, in a wireless manner, by an interrogator. In some embodiments, the transmitters 320 are defined by transceivers capable of receiving as well as transmitting. The "extinguisher" initiates a communication sequence, using a transmitter 320, when an alarm condition occurs. Each transmitter 320 is associated with or supported from a fire extinguisher 12 and coupled to the sensors 314, 316, and 318 associated with that fire extinguisher 312. The transmitters 320 are each configured to selectively transmit information identifying the fire extinguisher with which the transmitter is associated and to selectively transmit information indicating what the sensors 314, 316, or 318 are sensing. In some embodiments, the transmitters 320 are defined by, for example, a 915 MHz or other band RF transceiver. These are small, inexpensive, systems with a predetermined range (e.g., about 300 feet of range). In addition, they are low enough in power not to require FCC licensing. An example of the type of technology presently available is the uD3 system used to monitor urban power meters. The uD3 system is described at www.udatanet.com.

[0140] In some embodiments, at least some of the transmitters 320 are defined by radio frequency identification devices 322 that respectively include

transmitter 320, a processor 324 coupled to the transmitter 320, and a battery 326 coupled to the transmitter 320 and processor 324 to supply power to the transmitter 320 and processor 324. Batteries are readily available that can operate the system 310 for over five years, for example, if the extinguishers are polled just a few times each month. A typical battery is, for example, a 3.7volt 350mA hour lithium battery.

[0141] The radio frequency identification devices 322 each include a common housing 328 supporting or enclosing the transmitter 320, processor 324, and, in some embodiments, the battery 326. The radio frequency identification devices 322 are configured to selectively identify themselves to the receiver. For example, the radio frequency identification devices 322 can be of a design as described in one or more of the following commonly assigned patent applications, which are incorporated herein by reference: U.S. Patent Application Attorney Serial No. 10/263,826, filed October 2, 2002, entitled "Radio Frequency Identification Device Communications Systems, Wireless Communication Devices, Wireless Communication Systems, Backscatter Communication Methods, Radio Frequency Identification Device Communication Methods and a Radio Frequency Identification Device" by inventors Michael A. Hughes and Richard M. Pratt; U.S. Patent Application Serial No. 10/263,809, filed October 2, 2002, entitled "Method of Simultaneously Reading Multiple Radio Frequency Tags, RF Tag, and RF Reader", by inventors Emre Ertin, Richard M. Pratt, Michael A. Hughes, Kevin L. Priddy, and Wayne M. Lechelt; U.S. Patent Application Serial No. 10/263,873, filed October 2, 2002, entitled "RFID System and Method Including Tag ID Compression", by inventors Michael A. Hughes and Richard M. Pratt; U.S. Patent Application Serial No. 10/264,078, filed

October 2, 2002, entitled "System and Method to Identify Multiple RFID Tags", by inventors Michael A. Hughes and Richard M. Pratt; U.S. Patent Application Serial No. 10/263,940, filed October 2, 2002, entitled "Radio Frequency Identification Devices, Backscatter Communication Device Wake-Up Methods, Communication Device Wake-Up Methods and A Radio Frequency Identification Device Wake-Up Method", by inventors Richard Pratt and Michael Hughes; U.S. Patent Application Serial No. 10/263,997, filed October 2, 2002, entitled "Wireless Communication Systems, Radio Frequency Identification Devices, Methods of Enhancing a Communications Range of a Radio Frequency Identification Device, and Wireless Communication Methods", by inventors Richard Pratt and Steven B. Thompson; U.S. Patent Application Serial No. 10/263,670, filed October 2, 2002, entitled "Wireless Communications Devices, Methods of Processing a Wireless Communication Signal, Wireless Communication Synchronization Methods and a Radio Frequency Identification Device Communication Method", by inventors Richard M. Pratt and Steven B. Thompson; U.S. Patent Application Serial No. 10/263,656, filed October 2, 2002, entitled "Wireless Communications Systems, Radio Frequency Identification Devices, Wireless Communications Methods, and Radio Frequency Identification Device Communications Methods", by inventors Richard Pratt and Steven B. Thompson; U.S. Patent Application Serial No. 10/263,635, filed October 4, 2002, entitled "A Challenged-Based Tag Authentication Model", by inventors Michael A. Hughes and Richard M. Pratt; U.S. Patent Application Serial No.09/589,001, filed June 6, 2000, entitled "Remote Communication System and Method", by inventors R. W. Gilbert, G. A. Anderson, K. D. Steele, and C. L. Carrender; U.S. Patent Application Serial No. 09/802,408; filed March 9, 2001, entitled "Multi-

Level RF Identification System"; by inventors R. W. Gilbert, G. A. Anderson, and K. D. Steele; U.S. Patent Application Serial No. 09/833,465, filed April 11, 2001, entitled "System and Method for Controlling Remote Device", by inventors C. L. Carrender, R. W. Gilbert, J. W. Scott, and D. Clark; U.S. Patent Application Serial No. 09/588,997, filed June 6, 2000, entitled "Phase Modulation in RF Tag", by inventors R. W. Gilbert and C. L. Carrender; U.S. Patent Application Serial No.09/589,000, filed June 6, 2000; entitled "Multi-Frequency Communication System and Method", by inventors R. W. Gilbert and C. L. Carrender; U.S. Patent Application Serial No. 09/588,998; filed June 6, 2000, entitled "Distance/Ranging by Determination of RF Phase Delta", by inventor C. L. Carrender; U.S. Patent Application Serial No. 09/797,539, filed February 28, 2001, entitled "Antenna Matching Circuit", by inventor C. L. Carrender; U.S. Patent Application Serial No. 09/833,391, filed April 11, 2001, entitled "Frequency Hopping RFID Reader", by inventor C. L. Carrender. The advantages of selecting any of the designs are the same as the advantages suggested in the respective patent applications.

[0142] In some embodiments, the microprocessor 324 is a simple, low cost, 8-bit micro controller that monitors the three sensors 314, 316, 318 and send/receive commands from the transceiver 320. An ID code is stored in nonvolatile memory of the microprocessor 324, thus uniquely identifying the extinguisher. In some embodiments, additional locations in the nonvolatile memory, or additional memory, is used to store the maintenance record, and location of the extinguisher.

[0143] The system 310 further includes a receiver 330 in selective wireless communications with the transmitters 320. In some embodiments, the receiver 330 is defined by a transceiver.

[0144] The system 310 further includes a computer 332 coupled to the receiver. In some embodiments, the computer 332 is configured to maintain testing schedules for respective fire extinguishers 312 in, for example, a maintenance database 334. In some embodiments, the computer 332 is configured to provide an output when it is time for an extinguisher 312 to be inspected, tested, and/or undergo maintenance. For example, the computer 332 includes an alarm system 335 defined, for example, by a monitor configured to provide visual information or alerts and/or a speaker configured to provide audible information.

[0145] The computer 332 is also configured to selectively store information from a plurality of the transmitters 320. More particularly, the computer is configured to selectively store information from the sensors 314, 316, and 318 coupled to a transmitter 320 as well as information identifying the transmitter 320 and/or the fire extinguisher 312 to which the transmitter 320 is attached. The information is stored, for example, in maintenance database 334.

[0146] In some embodiments, the computer 332 contains all of the records also recorded in the individual extinguishers 312 to meet fire protection system standards/requirements. Thus, maintenance records, histories, charging status, etc., are stored in two locations--in the computer 332 and in the memory of the microprocessors 324 associated with the various fire extinguishers 312. In some embodiments, the computer 332 is interfaced to an alarm panel containing a map of the extinguishers location, and thus can indicate when an event

occurred, what extinguisher it was, and its location. In some embodiments, operators of the computer 332, such as Safety/ Security Managers may use the computer to poll individual extinguishers 312 to ascertain operability of the extinguisher, as well as determine condition/status radio frequency identification device system components, i.e., transmitters 320, transceivers 330, micro-processors 324, and battery units 326. This will permit Safety/Security Managers to be alerted to and address anomalies that may be developing in regard to these system components, prior to a component actually malfunctioning.

[0147] In some embodiments, at least one of the transmitters 320 is configured to communicate with the receiver 330 (see Fig. 22) via another of the transmitters 320. More particularly, one or more of the transmitters 320 are configured to communicate in a daisy-chain fashion.

[0148] In alternative embodiments, a radio frequency identification device 322 is used to define one of the transmitters 320 and also define a sensor. For example, in one embodiment, a radio frequency identification device 322 is used to define one of the transmitters 320 and also define a sensor 14 to sense if the associated fire extinguisher 312 is moved. In these embodiments, the radio frequency identification device 322 includes a conductor 336 configured to be broken in response to movement of the associated fire extinguisher 312. In some embodiments, the radio frequency identification device 322 includes frangible material including a conductor 336 configured to be broken in response to movement of the associated fire extinguisher 312. The conductor 336 can be arranged in a manner similar to the manner in which conductor 80, 80', etc. is

arranged as described above in connection with Fig. 5, 5A, 5B, 6A, 6B, 6C, 7, 8, 9, 10, 11, 12 or 13, for example.

[0149] Thus, a system has been provided that allows for the remote monitoring of fire extinguishing equipment/protection systems within areas governed by standards/requirements established by Underwriters Laboratories, the National Fire Protection Association (NFPA), and/or the Occupational Safety and Health Administration (OSHA). The system helps ensure building/facility Safety/Security Managers are immediately alerted/notified to anomalies relating to tamper, theft, operability of fire extinguishers, and to enhance/ensure the timely inspection, testing, maintenance, management, record keeping of these systems, as well as potential anomalies that may be developing in regard to radio frequency identification devices.

[0150] The system makes it possible for Safety/Security Managers to remotely monitor the status of fire extinguishers to help ensure, 1) they are in their designated locations, 2) immediate altering in the event of tampering/theft, 3) immediate alerting in the event an extinguisher's pressure gauge reading/indicator falls below the operable range/position, 4) immediate alerting when an extinguisher is required to undergo scheduled inspection/testing/maintenance, and/or 5) timely record keeping of these systems. Various aspects of the invention provide building/facility Safety/Security Managers a reliable and cost effective way to ensure fire extinguishers are available, serviceable, and operational in the event of an emergency.

[0151] A human no longer needs to manually inspect every extinguisher. In addition, should tampering, a loss of pressure, etc., occur, the central

computer can immediately indicate an alarm condition. Existing fire extinguishing systems can be retrofitted with the sensor technology disclosed herein.

[0152] Because each extinguisher "tag" will has its own unique address, multiple extinguishers can communicate with the central computer, and indeed with each other. Thus, extinguishers can communicate in daisy chain to relay information to their nearest neighbor so that even remote extinguishers can get information to the central computer even though they are out of 300 feet of range, i.e., they only need to be within 300 feet of a tagged extinguisher as long as there is an eventual path to the central computer.

[0153] In compliance with the statute, the invention has been described in language more or less specific as to structural and methodical features. It is to be understood, however, that the invention is not limited to the specific features shown and described, since the means herein disclosed comprise preferred forms of putting the invention into effect. The invention is, therefore, claimed in any of its forms or modifications within the proper scope of the appended claims appropriately interpreted in accordance with the doctrine of equivalents.